The President's National Security Telecommunications Advisory Committee

R&D Exchange
Human Factors Breakout Session

Mr. Michael Vatis, Dartmouth University
Ms. Marisa Reddy, Secret Service

March 14, 2003

Human Factors: Issues of Interest

- **Prevention: minimizing risk of inadvertent failures and malicious acts**
  - **Training and policy development, dissemination, and enforcement**
  - **Technology solutions (e.g., "secure by default," security templates)**
  - **Human responses to technical information (e.g., alerts)**
  - **Anomaly detection**
  - **Psychology/motivations of insiders**
- **Cultural shift**
  - **Corporate governance (e.g., accountability, enforcement from top to bottom)**
  - **Public awareness and education (embracing security from the bottom up)**
- **Source of Supply: minimizing risk, given growing dependence of U.S. on COTS**
  - **Code checking technologies**
  - **Self-healing (or self-correcting) technologies**
  - **Background checks (of individuals and/or companies)**

Human Factors: Impediments

- **Assumptions about balancing security with …**
  - **Privacy and other policy concerns**
  - **Good technology**
  - **Ease of use**
- **Identifying key business drivers**
- **Articulating/quantifying value of security**
  - **"No matter the sophistication of the technology or its simplicity of use, they create an additional burden (investment or maintenance costs)"**
- **Addressing legal, definitional, and cultural issues**
  - **Creating an environment where industry and government share data, report crimes**
  - **What is the definition of NS/EP in today's context?**

Human Factors: Most Pressing Research Areas

- **Making Security Easier**
  - Leverage knowledge from other disciplines to minimize biases and risks related to information security
  - Enhance decision making under uncertainty
  - Reduce impact of human factors (e.g., number of humans interfacing with key systems) by making security transparent
- **Anomaly Detection**
  - Research automated tools/techniques to detect anomalies (physical access and cyber) across an entire enterprise
  - Enhance tools to better visualize/refine the outputs from detection system
- **Education, Training, and Awareness**
  - Educate, train, and increase awareness of security issues (e.g., market research for different demographics)

Human Factors: Most Pressing Research Areas

- **"Insider Threat" Research**
  - **Investigate true prevalence of insider incidents**
  - **Research cultural, psychological, technical, and organizational factors that motivate and deter insiders**
  - **Research tools and techniques to better combat insider threat**
  - **Translate insider threat research (existing/ongoing) into useful techniques and policies**
- **Supply Source**
  - **Explore avenues for distributing tasks for checking source code (possible coordination through Centers of Excellence)**
  - **Validate distribution processes**
  - **Prioritize what code needs to be checked**

Human Factors: Out of the Box Thinking

- **Explore paradigm-shifting research in other sectors (e.g., health care, weather forecasting) that might offer new insights into information security**
- **Research useable, cost effective, and interoperable multi-layer technologies for authentication and authorization**
- **Research ways to identify suppliers whose products may pose a threat to NS/EP information systems**
- **Create a market for security (e.g., tax incentives, certification of companies as secure, public filing)**
- **Research on offensive tactics and strategies for information security**